Available online at http://www.ijasrd.org/in

International Journal of Advanced Scientific Research & Development

Vol. 03, Iss. 01, Ver. II, Jan – Mar' 2016, pp. 126 – 133

e-ISSN: 2395-6089
p-ISSN: 2394-8906

ENHANCING SECURITY THROUGH DATA HIDING

E. Sankari[1]
R. Shanmuga Priya[1]
R. Suriya[1]

[1] Final Year Students, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

G. Prabhakaran[2]
T. Sowkarthika[2]

[2] Assistant Professor, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

ARTICLE INFO

Article History:

Received: 08 Mar 2016;
Received in revised form:
13 Mar 2016;
Accepted: 13 Mar 2016;
Published online: 31 Mar 2016.

Key words:

AES,
RDH (Reversible Data Hiding),
Stegnography,
Cover Image

ABSTRACT

The use of computer networks for data transmissions has created the need of security. The security of this interactive media information can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. They send Secret message over channel using Cryptography and Steganography algorithms by AES (Advanced Encryption Standard). It is used to encrypt the data from plain text to cipher text vice versa. There are two types of keys available in the cryptography, symmetric and asymmetric. There are using symmetric key which is divided into two key such as private and public key. Public key is used for encryption and private key is used for decryption. The reversible data hiding technique is used to retrieve the data and image separately and securely. By using three types of keys it is more secure than other techniques. Steganography is the technique which is used in cryptography for more secure purpose. They are using local host path for data transmission.

How to cite this article: Sankari, E., Priya, S. R., Suriya, R., Prabhakaran, G., & Sowkarthika, T., (2016). "Enhancing Security through Data Hiding". *International Journal of Advanced Scientific Research & Development (IJASRD), 03* (01/II), pp. 126 – 133.

INTRODUCTION

It propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. "Reserve room before encryption", we first empty out room by embedding LSBs of some pixels into other pixels with a traditional Stegno method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance. Reversible data hiding (RDH) in images is a technique, by which the original cover can be loss less recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest. In practical aspect, many Stegno techniques have emerged in recent years. Constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them loss less, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance. With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. In, advocated a reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data.

1.1 Stegnography:

Substitution methods substitute redundant parts of a cover with a secret message spatial domain. It is more robust as it is integrated with an Advanced Encryption Standard (AES).

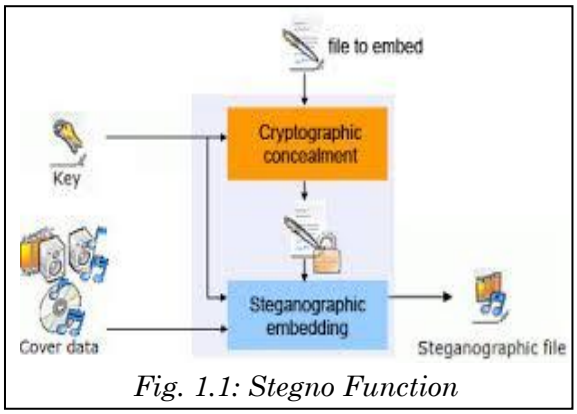


Fig. 1.1: Stegno Function

1.2 AES Algorithm:

An advanced Encryption standard is a symmetric-key encryption standard. It is fast in both hardware and software. Fixed block size is 128, 192, 256 bits. Substitution permutation is used. The cipher is specified as a number of

repetition of transformation rounds that convert the input plaintext into the final output of ciphertext. 1. Key Expansion, 2. Initial Round, 3. Round (sub bytes, shift rows, mix columns), and 4. Final Round (no mix columns)

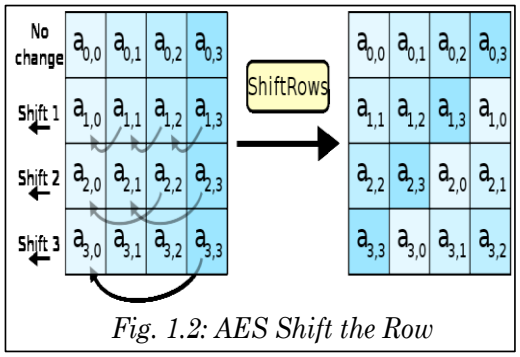


Fig. 1.2: AES Shift the Row

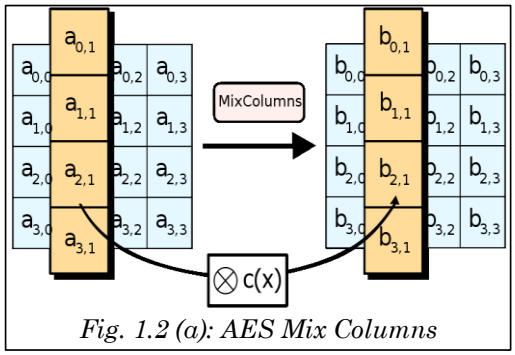
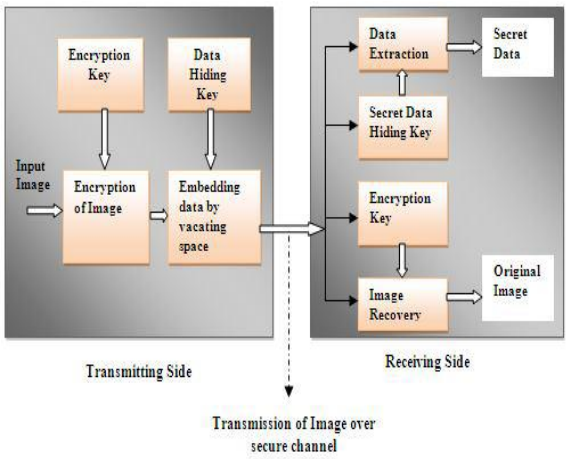


Fig. 1.2 (a): AES Mix Columns

1.3 RDH:

Reversible data hiding can be defined as an approach where the data is hidden in the host media that may be a cover image. A reversible data hiding is an algorithm, which can recover the original image lossless after the data have been extracted.

Fig 1.3: *RDH Technique*



MODULES DESCRIPTIONS

- User Management
- Encryption
  - Encrypt Image
  - Embed Data
  - Decryption
- Decrypt Image
  - De-embed Data
  - Decrypt image and de-embed data

EXPERIMENTAL RESULT

To create Database and store all the data, it can be registered to design the database.

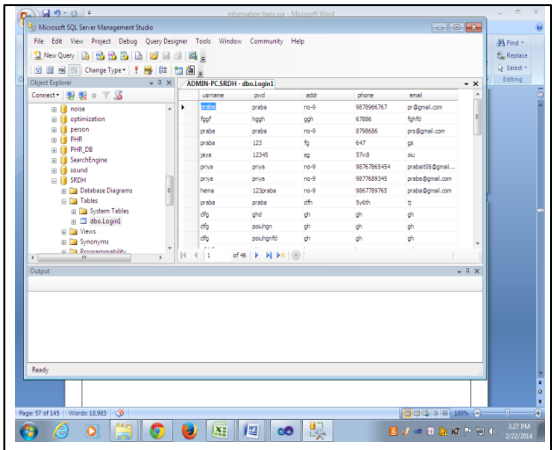


Fig 3(a) database creation

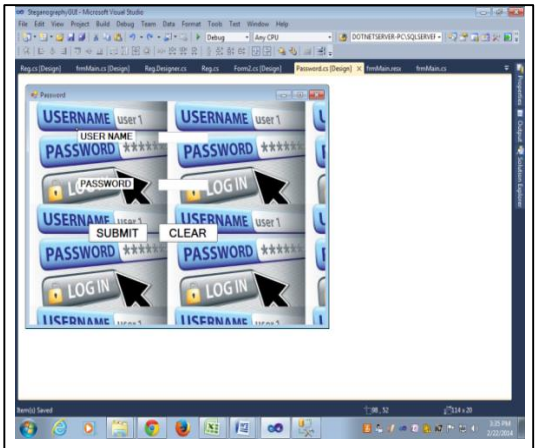


Fig 3(b) Registration

3.1 User Management:

User can create account by registering into the server. A user can log in to obtain access and can then log out or log off, when the access is no longer needed.

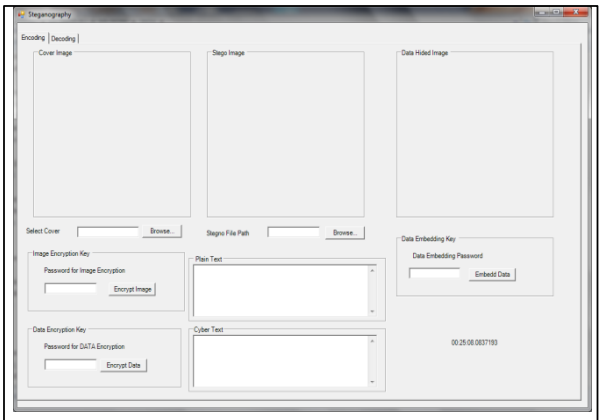


Fig 3.1 open user management page

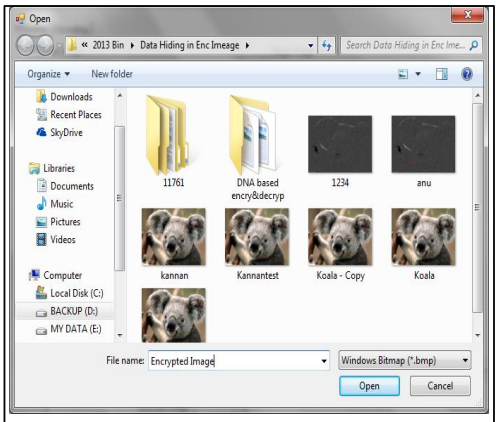


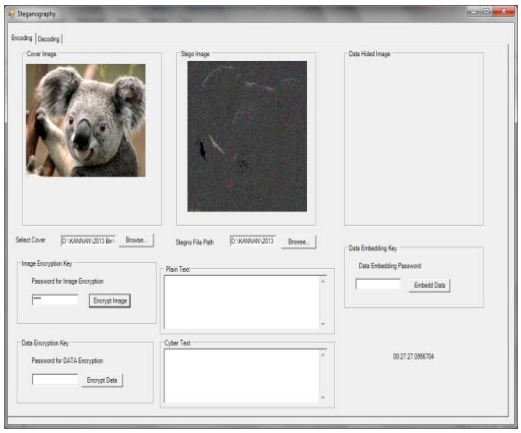
Fig 3.1(a) select bmp image

3.2 Encryption:

3.2.1 Encrypt Image:

The input image is encrypted using an encryption key before the compression of image. By which can an image is restricted to view from the unauthorised user access.

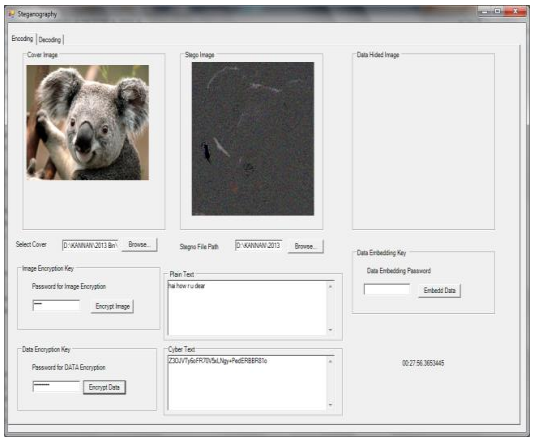
Fig 3.1.1: *encrypt image*



3.2.2 Encrypt Data:

The Secret data can be embedded using data encryption key. The encrypted data can be sending to channel for authentication.

Fig 3.1.2: *Encrypt Data*



3.2.3 Embed Data:

In the image the data is embedded after compressing the image by using appropriate technique. The message is embed in to the picture utilizing information covering up key.

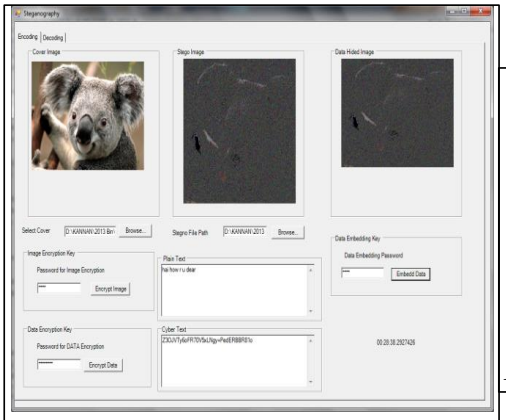


Fig 3.1.3 hiding the data into image

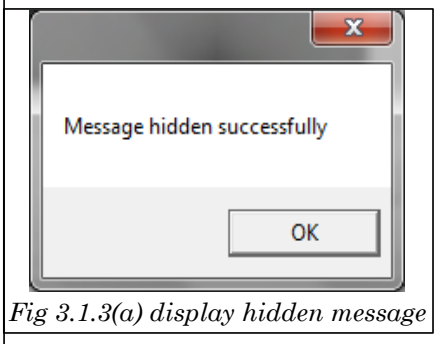
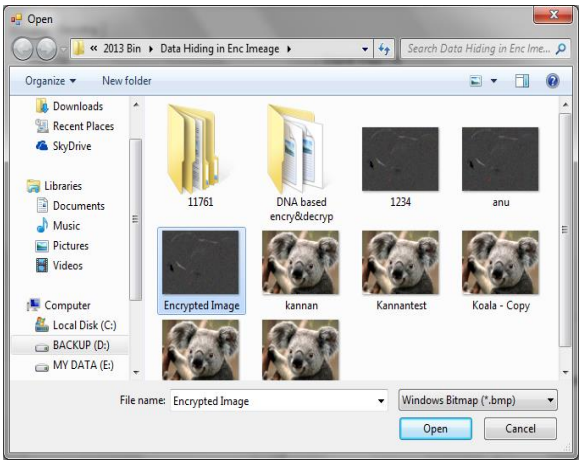


Fig 3.1.3(a) display hidden message

3.3 Decryption:

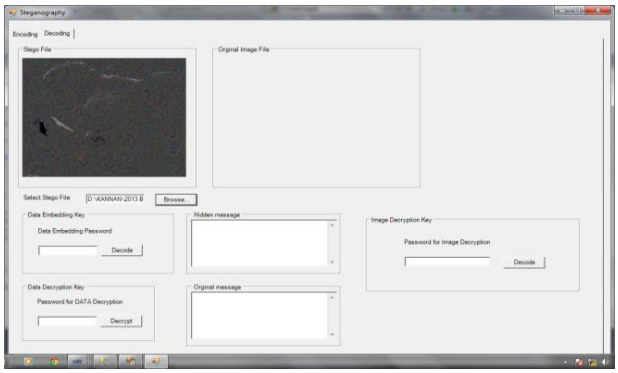
Fig 3.2: *Select the Encrypt Image*



3.3.1 Decrypt Image:

The image is decrypted using the encryption key used for encryption of the image. By using the encryption key a user can only access to the image Content.

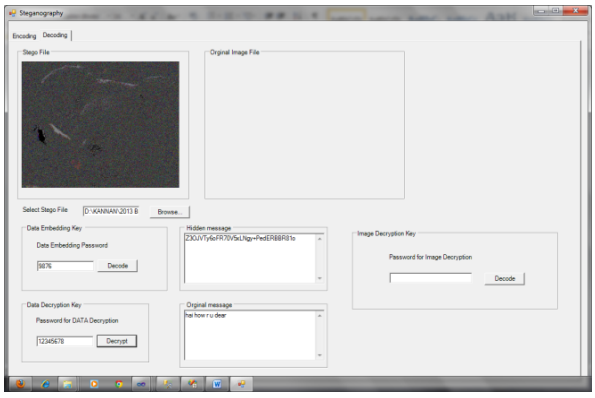
Fig 3.2.1: *Decrypt Image*



3.3.2 De-embed Data:

The data is extracted using the data hiding key used for the hiding the data into the image. By using the data hiding a user can access only to the data within the encrypted image.

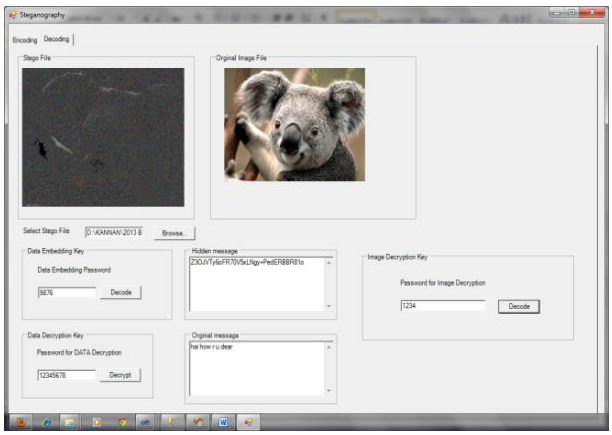
Fig 3.2.2: *Decrypted Data*



3.4 Decrypt image and de-embed data:

A user who has the both encryption key and data hiding key can access to the image and to the data hidden within the image both.

Fig 3.3: *Original Data*



CONCLUSION

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

REFERENCES

[1] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.

[2] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Jan. 2011.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W.Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[4] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[5] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[6] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[7] Priya Thomas and Avanish Kumar Singh, "A Novel Steganographic Approach for Enhancing the Security of Images", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, June 2013, pg.209 – 215.

[8] C. Anuradha and S. Lavanya, "Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, pp. 1009 - 1014, April 2013.

[9] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Transactions on Information Forensics and Security, Volume 8 Issue 3, pp. 553-562, March 2013.

[10] Lalit Dhande, Priya Khune, Vinod Deore, and Dnyaneshwar Gawade, "Hide Inside-Separable Reversible Data Hiding in Encrypted Image", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 3, Issue 9, pp. 88 - 91, February 2014

[11] Ann Mary Thomas and Binson. V. A. "Room Reserved Reversible Data Hiding in Encrypted Images", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Special Issue 1, pp. 208 - 215, March 2015.

[12] Sreekumar, S., & Salam, V. (2014). Advanced reversible Data Hiding With Encrypted Data. CoRR, abs/1408.0733.

[13] K. S. Sunitha, E. U. Iniyan and M. Moorthi, "Reversible Encrypted Data Concealment in Encrypted Images by Reserving Room approach for Data Protection System", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, pp. 1 - 5, Oct-Nov, 2013.

[14] Priya Kumar Jambhulkar, "Secure Reversible Data Hiding in Encrypted Images by Allocating Memory before Encryption via Security keys", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, pp. 491 - 497, March 2014.

[15] Chaple Gopal and G. Balram, "Reversible Data Hiding in Encrypted Images", International Journal of Science and Research (IJSR), Volume 3 Issue 9, pp. 762 - 767, Sep 2014.

[16] C. P. Sumathi, T. Santanam and G. Umamaheswari., "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, pp. 9 - 25, December 2013, doi: 10.5121/ijcses.2013.4602.

[17] Shruti M. Rakhunde "Reversible Data Hiding using Visual Cryptography: A Review", International Journal of Innovative Research in Computer and Communication Engineering, Retrieved from https://www.rroij.com/open-access/reversible-data-hiding-using-visual-cryptography-areview.php?aid=45014.

[18] E. Diana Jenifer and G. Swetha, "Encrypted Data Hiding in Video Stream using Code Word Substitution", IJSTE - International Journal of Science Technology & Engineering, Volume 1, Issue 9, pp. 39 - 45, March 2015.